(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 35 18 462 A1**

(51) Int. Cl. 4: H 04 L 9/02

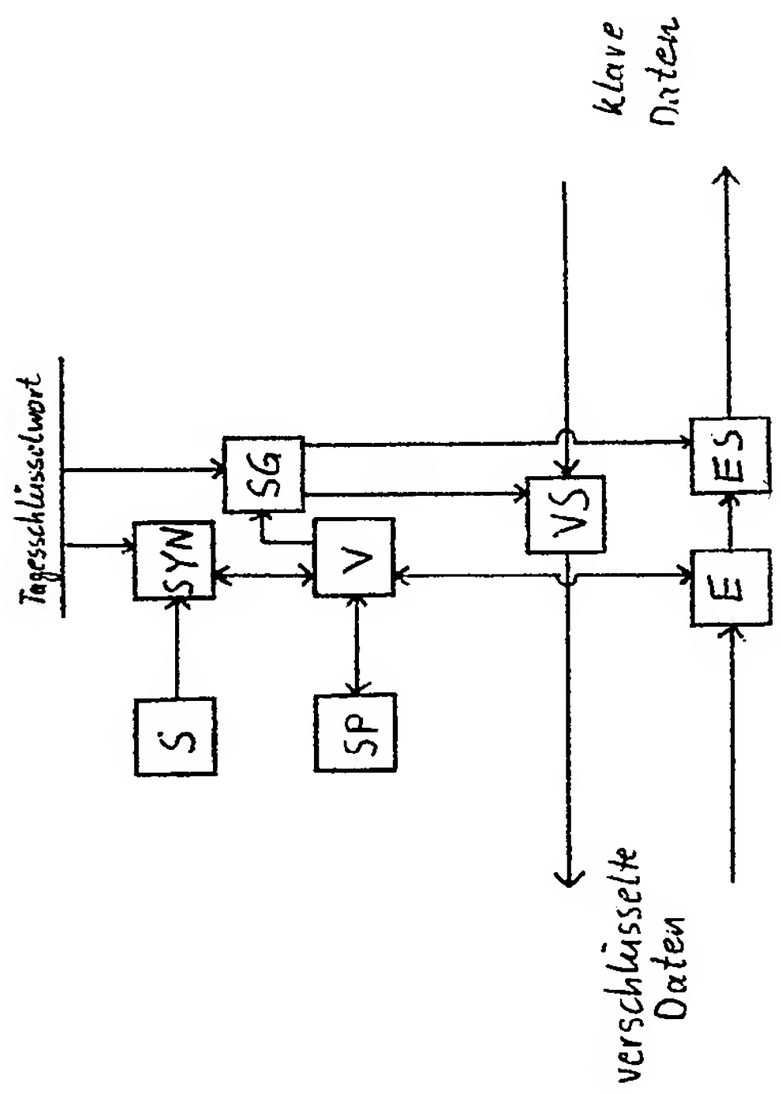
(21) Aktenzeichen: P 35 18 462.0
(22) Anmeldetag: 23. 5. 85
(43) Offenlegungstag: 27. 11. 86

(71) Anmelder:
Standard Elektrik Lorenz AG, 7000 Stuttgart, DE

(72) Erfinder:
Erbes, Norbert, Dr.-Ing., 7500 Karlsruhe, DE; Rother, Dietrich, Dr.-Ing., 7146 Tamm, DE

(54) System zur verschlüsselten Nachrichtenübertragung

Es wird ein System zur verschlüsselten Informationsübertragung angegeben, bei dem Recording-Störungen unterdrückt werden. Die Verschlüsselung erfolgt durch eine periodisch wiederkehrende Pseudo-Noise-Folge (Tagesschlüsselwort). Die erforderliche Synchronisation zwischen Sender und Empfänger erfolgt durch ein Synchronisationswort. Während der Gültigkeitsdauer des Tagesschlüsselwortes wird jedes Synchronisationswort nur einmal verwendet. Zumindest die bereits verwendeten Synchronisationsworte oder aus diesen abgeleitete Informationen sind in einem Synchronisationswortspeicher SP gespeichert. Tritt ein Synchronisationswort zweimal auf, so handelt es sich um eine Recording-Störung und die dazugehörende Information wird unterdrückt.



DE 35 18 462 A1

STANDARD ELEKTRIK LORENZ
AKTIENGESELLSCHAFT
S t u t t g a r t

N. Erbes - D. Rother 5-5

Patentansprüche

1. System mit mindestens zwei Sende/Empfangsstationen zur verschlüsselten digitalen Informationsübertragung, bei dem jede Station einen Schlüssler für die sendeseitige Verschlüsselung und die empfangsseitige Entschlüsselung mittels eines durch ein Tagesschlüsselwort einstellbaren PN-Generators enthält, dessen Startposition zu Beginn einer Informationsübertragung durch ein Synchronisationswort festgelegt wird, d a d u r c h g e k e n n z e i c h n e t , daß jede Station eine Schaltung mit einem Synchronisationswortspeicher SP enthält, in dem zumindest jedes verwendete Synchronisationswort gespeichert ist, daß die Schaltung jedes neu auftretende Synchronisationswort mit den bereits gespeicherten vergleicht und bei Gleichheit sendeseitig die Verwendung eines noch nicht verwendeten Synchronisationswortes auslöst und empfangsseitig die dem Synchronisationswort folgende Nachricht unterdrückt.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die Synchronisationsworte in Abhängigkeit vom jeweils gültigen Tagesschlüsselwort erzeugt sind.

N. Erbes - D. Rother 5-5

3. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei Eingabe des gültigen Tagesschlüsselwortes in allen Stationen nach demselben Algorithmus eine Anzahl von Synchronisationsworten erzeugt und in derselben Reihenfolge im Synchronisationswortspeicher abgelegt werden.

4. System nach Anspruch 3, dadurch gekennzeichnet, daß mindestens zu Beginn einer Informationsübertragung die Speicheradresse des verwendeten Synchronisationswortes übertragen wird.

5. System nach Anspruch 3, dadurch gekennzeichnet, daß mindestens zu Beginn einer Informationsübertragung eine aus dem verwendeten Synchronisationswort abgeleitete Synchronisationsinformation übertragen wird.

6. System nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß im weiteren Verlauf der Informationsübertragung, sofern diese im Gegensprech-Betrieb erfolgt, keine Speicheradresse oder Synchronisationsinformation mehr übertragen wird, sondern nach jedem Richtungswechsel das jeweils folgende, noch nicht verwendete, im Synchronisationswortspeicher abgelegte Synchronisationswort verwendet wird.

N. Erbes - D. Rother 5-5

System zur verschlüsselten Nachrichtenübertragung

Die Erfindung bezieht sich auf ein System gemäß dem Oberbegriff des Anspruchs 1. Ein derartiges System ist aus der DE-OS 31 50 254 bekannt.

Zur Verschlüsselung von digitalen Nachrichten werden periodisch wiederkehrende Pseudo-Noise(PN)-Folgen verwendet. Zu Beginn einer Nachrichtenübertragung müssen die PN-Folgen der miteinander verkehrenden Stationen synchronisiert werden, d.h. sie müssen innerhalb der Periode den gleichen Startpunkt haben. Deshalb erzeugt der Sender ein Synchronisationswort, stellt es der verschlüsselten Nachricht voran und übertragt das Resultat zum Empfänger.

Vor allem bei drahtloser Nachrichtenübertragung hat ein Störer die Möglichkeit, eine vollständige Übertragung einschließlich des Synchronisationswortes aufzuzeichnen und später wieder auszusenden. Die Empfänger können die Sendung wieder entschlüsseln. Der Bediener der Empfangsstation kann dadurch erheblich getäuscht werden. Diese Art der Störung wird "Recording Störung" genannt.

Es ist Aufgabe der Erfindung, ein System der eingangs genannten Art anzugeben, das gegen "Recording Störungen" gewappnet ist.

N. Erbes - D. Rother 5-5

Diese Aufgabe wird durch die im Anspruch 1 genannten Merkmale gelöst. Vorteilhafte Weiterbildungen sind in den Unteransprüchen enthalten.

Die Erfindung hat den Vorteil, daß ohne nennenswerten Mehraufwand die Sicherheit der Informationsübertragung erhöht werden kann, indem nur eine das verwendete Synchronisationswort kennzeichnende Information nicht aber das Synchronisationswort selbst übertragen wird. Im Gegensprechbetrieb mit schnellem Richtungswechsel kann sogar auf die Übertragung einer derartigen Information verzichtet werden.

Die Erfindung wird nachstehend anhand dreier Ausführungsbeispiele erläutert.

Die einzige Figur zeigt ein Blockschaltbild der erfindungswesentlichen Teile einer Sende/Empfangsstation.

Jede Sende/Empfangsstation zur drahtlosen oder drahtgebundenen Nachrichtenübertragung - im folgenden ohne Beschränkung der Allgemeinheit Funkgerät genannt - enthält gemäß der Figur einen Synchronisationswortgenerator SYN und einen Schlüsselbitgenerator SG, in die ein Tagesschlüsselwort eingegeben werden kann. Der Synchronisationswortgenerator SYN ist an die Sendetaste S des Funkgeräts angeschlossen und ferner mit einem Vergleicher V verbunden. Der Vergleicher V ist mit einem Synchronisationswortspeicher SP, einer Einrichtung E und dem Schlüsselbitgenerator SG verbunden. Der Einrichtung E ist ein Entschlüssler ES nachgeschaltet. Der Schlüsselbitgenerator SG ist mit dem Verschlüssler VS und dem Entschlüssler ES verbunden.

Beim ersten Ausführungsbeispiel wird beim Senden über die Sendetaste S in Abhängigkeit vom jeweils gültigen Tagesschlüsselwort die Erzeugung eines Synchronisationswortes im Synchronisationswortgenerator SYN initiiert. Das Synchronisationswort wird danach dem Vergleicher V zugeführt, der es mit den bereits im Synchronisationswortspeicher SP gespeicherten Synchronisationsworten vergleicht. Ist das Synchronisationswort bereits gespeichert, veranlaßt der Vergleicher V die Erzeugung eines anderen Synchronisationswortes im Synchronisationswortgenerator SYN. Das andere Synchronisationswort wird ebenfalls mit den im Synchronisationswortspeicher SP enthaltenen verglichen. Ist es dort noch nicht gespeichert, veranlaßt der Vergleicher V die Speicherung desselben und führt es außerdem dem Schlüsselbitgenerator SG zu. Der Verschlüssler VS beginnt daraufhin mit der Verschlüsselung, stellt das Synchronisationswort den verschlüsselten Daten voran und führt das Resultat einer Senderschaltung (in der Figur nicht dargestellt) zu.

Beim Empfang (eine Empfangsschaltung und eine Schaltung zur Regeneration der Empfangssignale sind ebenfalls in der Figur nicht dargestellt) werden die verschlüsselten Daten der Einrichtung E zugeführt. Dort wird das Synchronisationswort von den Daten getrennt und dem Vergleicher V zugeführt. Dieser vergleicht es mit den bereits im Synchronisationswortspeicher SP gespeicherten. Ist das empfangene Synchronisationswort noch nicht gespeichert, veranlaßt der Vergleicher dessen Speicherung und gibt

der Einrichtung E ein Signal, die empfangenen Daten an den Entschlüssler weiterzugeben. Im anderen Fall unterbleibt die Weitergabe der Daten an den Entschlüssler. Damit ist sichergestellt, daß eine von einem Störer aufgezeichnete und wiederausgesendete Information unterdrückt wird, da jedes bereits verwendete Synchronisationswort gespeichert ist und nur einmal verwendet werden darf.

Bei einem zweiten Ausführungsbeispiel werden nach Eingabe des jeweils gültigen Tagesschlüsselwortes in allen Funkgeräten nach demselben Algorithmus eine Anzahl von Synchronisationsworten erzeugt und in derselben Reihenfolge im Synchronisationswortspeicher SP abgelegt. Zu Beginn einer Informationsübertragung wird nicht das ganze Synchronisationswort, sondern nur die Speicheradresse, unter der dieses im Synchronisationswortspeicher SP abgelegt ist, übertragen. Im Gegensprech-Betrieb mit schnellem Richtungswechsel wird auch auf die Übertragung der Speicheradresse verzichtet. Stattdessen wird automatisch das jeweils folgende, zuvor noch nicht verwendete, im Synchronisationswortspeicher SP gespeicherte Synchronisationswort zur Ver- und Entschlüsselung verwendet.

Zur Verhinderung von Recording-Störungen ist bei diesem Ausführungsbeispiel ein zweiter Speicher vorzusehen. Jedem Speicherplatz des Synchronisationswortspeichers SP ist genau der Speicherplatz des zweiten Speichers zugeordnet, der dieselbe Adresse besitzt. Bei Verwendung

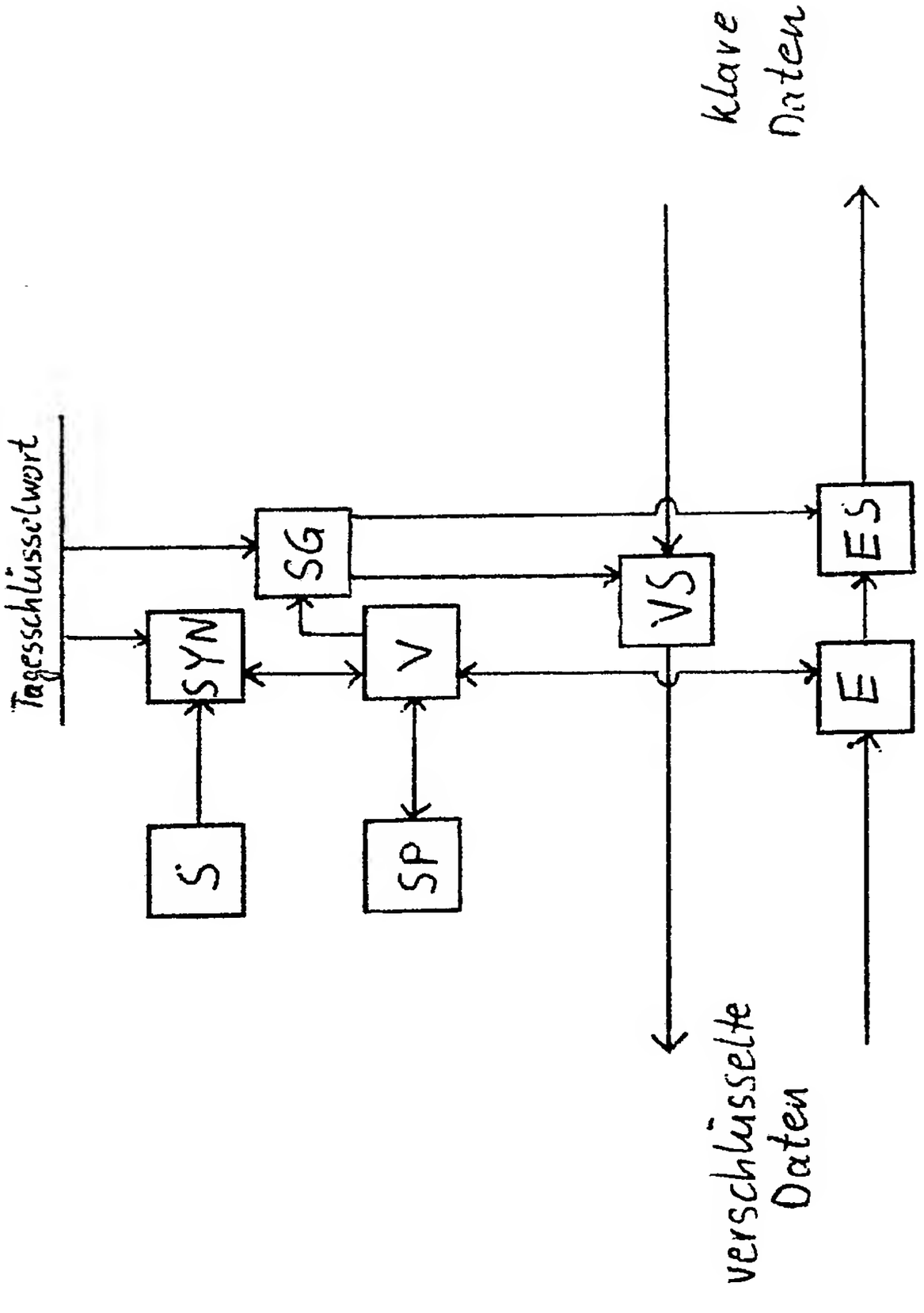
eines bestimmten Synchronisationswortes zur Informationsübertragung wird im zweiten Speicher der zugehörige Speicherplatz markiert (mit einer 0 oder 1). Um Recording-Störungen zu erkennen, muß der Vergleicher V nicht mehr die Synchronisationsworte vergleichen, sondern lediglich feststellen, ob im zugehörigen Speicherplatz des zweiten Speichers eine 0 oder 1 vorhanden ist. Dies geschieht in wenigen μsec.

Bei einem dritten Ausführungsbeispiel werden statt der Speicheradresse des zur Verschlüsselung verwendeten Synchronisationswortes eine aus dem Synchronisationswort nach einem Algorithmus, der vom Tagesschlüsselwort abhängen kann, abgeleitete Synchronisationsinformation übertragen. Diese Synchronisationsinformation, beispielsweise 16 Bit, wird als Adresse des zweiten Speichers verwendet, der wie beim zweiten Ausführungsbeispiel zur Markierung bereits verwendeter Synchronisationsworte dient. Da verschiedene Synchronisationsworte zur gleichen Synchronisationsinformation führen können, ist zwar die Anzahl der verfügbaren Synchronisationsworte geringer, die Übertragungssicherheit jedoch größer als beim zweiten Ausführungsbeispiel.

Tritt ein weiteres Funkgerät in einen bereits bestehenden Funkkreis ein, so ist die Möglichkeit vorhanden, die bereits verwendeten Synchronisationsworte abzufragen und in den Synchronisationswortspeicher SP des weiteren Funkgerätes einzuspeichern beziehungsweise die Markierung der bereits verwendeten durchzuführen.

Die Funkgeräte können um eine zusätzliche Schaltung erweitert werden, die das Auftreten von Recording-Störungen dem Bediener des Funkgeräts in geeigneter Form anzeigt.

Nummer: 35 18 462
Int. Cl.[4]: H 04 L 9/02
Anmeldetag: 23. Mai 1985
Offenlegungstag: 27. November 1986



Fig